Kapak Konusu: Geometrik Kombinatorik

Hadamard Matrisleri

Selda Küçükçifçi* / *skucukcifci@ku.edu.tr*

Her girdisi 1 ya da –1 olan ve $HH^t = n\mathrm{Id}_n$ eşitliğini sağlayan $n \times n$ boyutlu bir H matrisine n'lik ***Hadamard matrisi*** denir. Bu ifadede, Id_n, $n \times n$ lik birim matris, H^t de, H matrisinin devriğidir[1]:

$$\mathrm{Id}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\text{ve eğer } H = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \text{ ise } H^t = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix} \text{ dir.}$$

Aşağıda, 1, 2 ve 4'lük Hadamard matrislerine örnekler görüyorsunuz.

$$[1], \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Hadamard matrisleri özellikle kodlar teorisinde önemlidir, bu matrisler hata düzelten kodlar yaratmaya yarar.

$n \times n$'lik bir H matrisinin i-inci satırı ve j-inci sütunundaki (i, j) girdisini h_{ij} ile gösterirsek H^t matrisinin (i, j) girdisi aşağıda görüldüğü üzere h_{ji} olacağından,

$$H = \begin{pmatrix} h_{11} & \cdots & h_{1j} & \cdots & h_{1n} \\ \vdots & & \vdots & & \vdots \\ h_{i1} & \cdots & h_{ij} & \cdots & h_{in} \\ \vdots & & \vdots & & \vdots \\ h_{n1} & \cdots & h_{nj} & \cdots & h_{nn} \end{pmatrix} \quad H^t = \begin{pmatrix} h_{11} & \cdots & h_{i1} & \cdots & h_{n1} \\ \vdots & & \vdots & & \vdots \\ h_{1j} & \cdots & h_{ij} & \cdots & h_{nj} \\ \vdots & & \vdots & & \vdots \\ h_{1n} & \cdots & h_{in} & \cdots & h_{nn} \end{pmatrix}$$

HH^t matrisinin (i, j) girdisi, yan sütundaki hesapta görüldüğü gibi, $\sum_{k=1}^{n} h_{ik}h_{jk}$ dir. Ama tüm h_{ij} girdileri –1 ya da 1 ise, HH^t matrisinin (i, i) girdisi hep $\sum_{k=1}^{n} h_{ik}^2 = n$ olur. Dolayısıyla girdileri –1 ve 1 olan $n \times n$'lik bir matrisin Hadamard matrisi olması için gerek ve yeter koşul, her $1 \le i < j \le n$ için,

$$\sum_{k=1}^{n} h_{ik}h_{jk} = 0$$

eşitliğidir. Durup dururken bir teorem kanıtladık.

$$HH^t = \begin{pmatrix} h_{11} & \cdots & h_{1j} & \cdots & h_{1n} \\ \vdots & & \vdots & & \vdots \\ h_{i1} & \cdots & h_{ij} & \cdots & h_{in} \\ \vdots & & \vdots & & \vdots \\ h_{n1} & \cdots & h_{nj} & \cdots & h_{nn} \end{pmatrix} \begin{pmatrix} h_{11} & \cdots & h_{i1} & \cdots & h_{n1} \\ \vdots & & \vdots & & \vdots \\ h_{1j} & \cdots & h_{ij} & \cdots & h_{nj} \\ \vdots & & \vdots & & \vdots \\ h_{1n} & \cdots & h_{in} & \cdots & h_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} h_{11} & \cdots & h_{1k} & \cdots & h_{1n} \\ \vdots & & \vdots & & \vdots \\ h_{i1} & \cdots & h_{ik} & \cdots & h_{in} \\ \vdots & & \vdots & & \vdots \\ h_{n1} & \cdots & h_{nk} & \cdots & h_{nn} \end{pmatrix} \begin{pmatrix} h_{11} & \cdots & h_{j1} & \cdots & h_{n1} \\ \vdots & & \vdots & & \vdots \\ h_{1k} & \cdots & h_{jk} & \cdots & h_{nk} \\ \vdots & & \vdots & & \vdots \\ h_{1n} & \cdots & h_{jk} & \cdots & h_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} \sum_k h_{1k}^2 & \cdots & \sum_k h_{1k}h_{ik} & \cdots & \sum_k h_{1k}h_{jk} & \cdots & \sum_k h_{1k}h_{nk} \\ \vdots & & \vdots & & \vdots & & \vdots \\ \sum_k h_{ik}h_{1k} & \cdots & \sum_k h_{ik}^2 & \cdots & \sum_k h_{ik}h_{jk} & \cdots & \sum_k h_{ik}h_{nk} \\ \vdots & & \vdots & & \vdots & & \vdots \\ \sum_k h_{nk}h_{1k} & \cdots & \sum_k h_{nk}h_{ik} & \cdots & \sum_k h_{nk}h_{jk} & \cdots & \sum_k h_{nk}^2 \end{pmatrix}$$

HH^t matris çarpımı

Hadamard Dönüşümleri. Aynen latin kareler de olduğu gibi, bir Hadamard matrisinden başka Hadamard matrisleri elde edebiliriz.

Örneğin bir Hadamard matrisinin herhangi bir satırını ya da sütununu –1'le çarparsak yeni bir Hadamard matrisi elde ederiz. Bu dönüşümleri peşisıra uygulayarak, herhangi bir Hadamard matrisinden, ilk satırı ve ilk sütunundaki tüm girdileri 1 olan bir Hadamard matrisi yaratabiliriz. Bu özelliği taşıyan bir Hadamard matrisi ***standart Hadamard matrisi*** diye adlandırılır.

Bir Hadamard matrisinin iki satırının ya da iki sütununun yerlerini değiştirerek elde edeceğimiz matris de Hadamard matrisi olacaktır. Hatta satırları istediğimiz gibi, sıraları da istediğimiz gibi değiştirebiliriz, çıkan sonuç hep bir Hadamard matrisi olur.

Yukardaki işlemlerin kombinasyonlarını bir Hadamard matrisine uyguladığımızda elde edeceğimiz matris yine bir Hadamard matrisi olacaktır. Bu dönüşümlerle birbirinden türetilen matrislere ***denk*** Hadamard matrisleri denir.

Bir Hadamard matrisinin devriği[1] de (yani köşegene göre simetriği de) bir Hadamard matrisidir.

* Koç Üniversitesi Matematik Bölümü öğretim üyesi.

1 İngilizcesi "transpose".

Birbirine denk olmayan n'lik Hadamard matrislerinin sayısı sadece $n = 28$'e kadar belirlenebilmiştir. Sırasıyla $n = 4, 8, 12, 16, 20, 24, 28$ ise bu sayı 1, 1, 1, 5, 3, 60, 487'dir. Bu matrislerin listesine [Had1] internet adresinden ulaşabilirsiniz. Kai-Tai Fang ve Gennian Ge tam 382 tane denk olmayan 36'lık Hadamard matrisi olduğunu buldu. Daha var mı? Kimbilir!

Hadamard Matrislerinin Varlığı. Girişte 1, 2 ve 4'lük Hadamard matrisi örneği verdik ama 3'lük bir Hadamard matrisi vermedik. Bunun bir nedeni vardır: 3'lük Hadamard matrisi yoktur.

Hatta $n \neq 1$ tek ise n'lik bir Hadamard matrisi olamaz. Bunun kanıtı çok kolay: Bir Hadamard matrisi alalım. Sütunları gerektiğinde -1'le çarparak, ilk sıranın 1'lerden oluştuğunu varsayabiliriz. Şimdi, yukarda kanıtladığımız $\sum_{k=1}^{n} h_{ik}h_{jk} = 0$ eşitliğinde $i = 1$, $j = 2$ alalım: $\sum_{k=1}^{n} h_{2k} = 0$ buluruz. Her $h_{2k} = 1$ ya da -1 olduğundan, bundan, 1'e eşit olan h_{2k} girdilerinin sayısının -1'e eşit olan h_{2k} girdilerinin sayısına eşit olduğu anlaşılır. Demek ki n çift olmalı.

Peki $n = 6$ iken durum ne? Yanıt yine olumsuz:

Teorem 1. *n'lik Hadamard matrisi ancak $n = 1$, $n = 2$ ise ya da n, 4'ün bir katıysa olabilir.*

Kanıt: n, 2'den büyük olsun ve H, n'lik bir Hadamard matrisi olsun. H'nin standard olduğunu varsayabiliriz. Satırların yerlerini değiştirerek, H'nin ilk üç satırını

$$\begin{bmatrix} 1 & \cdots & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ 1 & \cdots & 1 & 1 & \cdots & 1 & -1 & \cdots & -1 & -1 & \cdots & -1 \\ 1 & \cdots & 1 & -1 & \cdots & -1 & 1 & \cdots & 1 & -1 & \cdots & -1 \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \end{bmatrix}$$

biçimine getirelim. Üçüncü satırın ilk yarısındaki 1'lerin sayısına a, -1'lerin sayısına b, ikinci yarısındaki 1'lerin sayısına c, -1'lerin sayısına d dersek, birinci ve ikinci satırların çarpımından,

$$a + b - c - d = 0,$$

birinci ve üçüncü satırların çarpımından,

$$a - b + c - d = 0,$$

ikinci ve üçüncü satırların çarpımından,

$$a - b - c + d = 0$$

eşitlikleri elde edilir. Bu eşitlikler $a = b = c = d$ eşitliklerini verir. Öte yandan uzunlukların toplamı n olduğundan $a + b + c + d = n$. Dolayısıyla $n = 4a$ ve n, 4'ün bir katı. □

Sanı: *4'ün katı olan her pozitif n tamsayısı için n'lik Hadamard matrisi vardır.*

Hadamard matrislerinin varlığı hakkında birçok sonuç elde edilmesine karşın bu sanı henüz kanıtlanamamıştır. Bu sanı kapsamında bilinen sonuçlardan birkaçını bu yazımızda ele alacağız. Bazılarından sadece sözedip, o sonuçlar için kaynak göstereceğiz, çünkü onları burada elde etmeye çalışmak için çok daha fazla tanım vermek ve daha karmaşık inşa yollarına girmek gerekiyor.

Bu konuda bilinmeyen birçok soru vardır. 428'lik Hadamard matrisi 2004'te Kharaghani ve Tayfeh-Rezaie tarafından bulunmuştur. Kaynaklarda şu anda bilinmeyen en küçük Hadamard matrisinin 668'lik Hadamard matrisi olduğu belirtilmekte. Siz bu satırları okurken belki de birileri bu matrisi elde etmiş olacaktır, ama 668'den büyük 4'e bölünen sayılar da vardır!

Şimdi kanıtı çok çok zor olmayan birkaç sonuç açıklayalım.

Teorem 2. *n ve r'lik Hadamard matrisleri varsa nr'lik Hadamard matrisi de vardır.*

Kanıt: K ve L sırasıyla n ve r'lik Hadamard matrisleri olsun. k_{ij}, K matrisinin (i, j) girdisi olsun. Aşağıdaki gibi $nr \times nr$ lik bir H matrisi tanımlayalım.

$$H = \begin{bmatrix} k_{11}L & k_{12}L & \dots & k_{1n}L \\ k_{21}L & k_{22}L & \dots & k_{2n}L \\ \dots : & \dots & \dots & \dots \\ k_{n1}L & k_{n2}L & \dots & k_{nn}L \end{bmatrix}$$

Matris çarpımı kurallarından, HH^t matrisinin (i, j) pozisyonunda $r \times r$ boyutlu

$$\textstyle\sum_{x=1}^{n} k_{ix}k_{jx}LL^t = (\sum_{x=1}^{n} k_{ix}k_{jx})r\mathrm{Id}_r$$

altmatrislerin olduğu anlaşılır.

$\sum_{x=1}^{n} k_{ix}k_{jx}$ sayısı $i = j$ ise n ve $i \neq j$ ise 0 olduğundan, $i = j$ ise (i, j) altmatrisi $nr\mathrm{Id}_r$'ye, diğer durumlarda 0 matrisine (tüm girdileri 0 olan matrise) eşittir. Böylece $HH^t = nr\mathrm{Id}_{nr}$ eşitliği bulunur. H'nin her girdisi 1 ya da -1 olduğundan, tanımlanan H bir Hadamard matrisidir. □

Sonuç 3. *Her k pozitif tamsayısı için 2^k'lik Hadamard matrisi vardır.*

Kanıt: 2'lik Hadamard matrisleri sayesinde bir önceki sonuç kullanılarak her k için 2^k'lık Hadamard matrisleri bulunabilir. □

Hadamard Matrisleri ve Tasarımlar. Gelelim tasarımlarla Hadamard matrisleri arasındaki ilişkiye... 2-(v, k, λ) tasarımları "Tasarımlar" yazısında tanımlanmıştı (sayfa 28.) $4m$'lik bir Hadamard matrisinden bir 2-($4m$–1, $2m$–1, m–1) tasarımı, 2-($4m$–1, $2m$–1, m–1) parametreli bir tasarımdan da $4m$'lik bir Hadamard matrisini elde edebiliriz. Bu yüzden 2-($4m$–1, $2m$–1, m–1) parametreli tasarımlara ***Hadamard tasarımları*** da denir.

Bunun kanıtına geçmeden önce bir örnek verelim: $m = 3$ olduğunda,

$$v = 4m - 1 = 11,$$
$$k = 2m - 1 = 5,$$
$$\lambda = m - 1 = 2$$

olur ve bu yöntem bize, eğer 2-(11, 5, 2) tasarımı varsa 12'lik bir Hadamard matrisi verir. Ama 2-(11, 5, 2) tasarımı örneğini sayfa 31'deki gri alanda görmüştük. Dolayısıyla 12'lik bir Hadamard matrisi de vardır.

Bir tasarımın ***oluşum matrisi***ni de aynı yazıda tanımlamıştık. Anımsatalım: Tasarımın bloklarını $\ell_1, ..., \ell_b$ olarak, noktalarını da $P_1, ..., P_v$ olarak sıralayıp $v \times b$ boyutlu oluşum matrisini şöyle tanımlayalım: A'nın i-inci sıra, j-inci sütundaki girdisi, eğer P_i noktası ℓ_j blokundaysa 1, değilse 0 olsun. Böylece, oluşum matrisinin her sütunu bir bloku temsil eder ve bir sütundaki 1'ler o sütunu temsil eden blokun noktalarını belirtir.

İstediğimiz sonucu kanıtlamadan önce 0 ve 1'lerden oluşmuş bir matrisin ne zaman bir tasarımın oluşum matrisi olacağını söyleyen cebirsel bir ifade bulalım.

$J_{v\times b}$ ve J_v tüm girdileri 1 olan sırasıyla $v \times b$ ve $v \times v$ boyutlu matris olsunlar.

Teorem 4. *$v \times b$ boyutlu bir A matrisinin bir 2-(v, k, λ) tasarımının oluşum matrisi olması için gerek ve yeter koşul* $AA^t = (r - \lambda)\mathrm{Id}_v + \lambda J_v$ *ve* $J_vA = kJ_{v\times b}$ *eşitliklerini sağlamasıdır.*

Kanıt: Önce A, bir 2-(v, k, λ) tasarımının oluşum matrisi olsun. Birinci eşitliği sayfa 52'de Teorem 2'de kanıtlamıştık. Matris çarpımı yapıldığında J_vA'nın girdilerinin doğruların üstünde bulunan nokta sayısı (yani k) olduğu hemen anlaşılır. Demek ki $J_vA = kJ_{v\times b}$ eşitliği doğrudur.

Şimdi girdileri 0 ve 1'ler olan bir A matrisinin önermede verilen iki eşitliği sağladığını varsayalım. Her 0-1 matrisi gibi A matrisi de bize bir çeşit "düzlem geometrisi" verir: Sütunları geometrinin blokları olarak, sıraları da noktaları olarak algılayalım. Böylece sütun sayısı kadar blok (b tane), sıra sayısı kadar da nokta (v tane) elde ederiz. Bir sütunda bulunan 1 ya da 0, o sayının bulunduğu sıraya eş düşen noktanın, o sütunu temsil eden doğruda olup olmadığını söyler. Böyle yorumlandığında, ikinci eşitlik, A'nın her blokunda k noktanın olduğu bir tasarımın oluşum matrisi olduğunu söyler. Birinci eşitlik ise herhangi iki farklı noktanın λ değişik blokta birlikte bulunduğunu ve her noktanın tam r blokta olduğunu söyler. □

Sonuç 5. *$4m$'lik Hadamard matrisinin varlığı için gerek ve yeter koşul* 2-($4m$–1, $2m$–1, m–1) *tasarımın varlığıdır.*

Kanıt: H, $4m$'lik standard bir Hadamard matrisi olsun. $j \neq 1$ için $\sum_{k=1}^{4m} h_{1k}h_{jk} = 0$ yani $\sum_{k=1}^{4m} h_{jk} = 0$. Aynı şekilde $j \neq 1$ için $\sum_{k=1}^{4m} h_{kj} = 0$. Demek ki ilk satır ve sütun haricinde diğer tüm satır ve sütunlardaki girdilerin toplamı 0. Şimdi H matrisinin ilk satır ve sütununu silip $(4m-1)\times(4m-1)$ lik bir A matrisi elde edelim. Aşağıda H ve H^t matrislerinin A ve A^t ile ilişkisini görüyorsunuz.

$$H = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & A & \\ 1 & & & \end{bmatrix}, H^t = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & A^t & \\ 1 & & & \end{bmatrix}$$

A matrisinin her satır ve sütunundaki girdilerinin toplamı −1 olacaktır, diğer bir deyişle

$$AJ = JA = -J.$$

(Bundan böyle J_{4m-1} yerine, kolaylık olsun diye, sadece J yazacağız.) Öte yandan $HH^t = 4m\mathrm{Id}_{4m}$, yani

$$4m\mathrm{Id}_{4m} = HH^t = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & A & \\ 1 & & & \end{bmatrix}\begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & A^t & \\ 1 & & & \end{bmatrix}$$
$$= \begin{bmatrix} 4m & * & \dots & * \\ * & & & \\ \vdots & & J + AA^t & \\ * & & & \end{bmatrix}.$$

Bu eşitlikten ilk satırı ve ilk sütunu silersek,

$$4m\mathrm{Id}_{4m-1} = J + AA^t$$

ya da

$$AA^t = 4m\mathrm{Id}_{4m-1} - J$$

buluruz. Yeni bir B matrisini şöyle tanımlayalım:

$$B = (A + J)/2.$$

Şimdi biraz daha hesap yapalım:

$$BJ = (AJ + J^2)/2 = ((-J + (4m-1)J)/2 = (2m-1)J.$$

$AJ = JA$ olduğundan, benzer şekilde,

$$JB = (2m - 1)J.$$

Ayrıca,

$$\begin{aligned} BB^t &= (A + J)(A^t + J)/4 \\ &= (AA^t + JA^t + AJ + JJ)/4 \\ &= ((4m\mathrm{Id} - J) - J - J + (4m - 1)J)/4 \\ &= m\mathrm{Id} + (m - 1)J. \end{aligned}$$

Bu eşitlikler B'nin 2-$(4m-1, 2m-1, m-1)$ tasarımın oluşum matrisi olduğunu gösterir.

Oluşum matrisini $C = (J - A)/2$ olarak tanımlarsak 2-$(4m - 1, 2m, m)$ tasarımını elde ederiz.

Kanıtı tersten ilerletir, 2-$(4m - 1, 2m - 1, m - 1)$ ya da 2-$(4m - 1, 2m, m)$ tasarımı ile başlar, 0 olan girdileri -1 ile değiştirirsek A ya da $-A$ matrislerini elde ederiz. □

Yazıyı teoremin iki önemli sonucuyla bitirelim:

1. Asal bir p ve k, m doğal sayıları için, $4m = p^k + 1$ ise, o zaman $4m$'lik bir Hadamard matrisi vardır. Bu sonuç, yukardaki teoremin uygulanacağı tasarımlar bulunarak kanıtlanır. İnşası biraz karmaşık olduğu için bu tasarımları bu yazımızda açıklayamayacağız ama ilgili okur [WSW]'ye bakabilir.

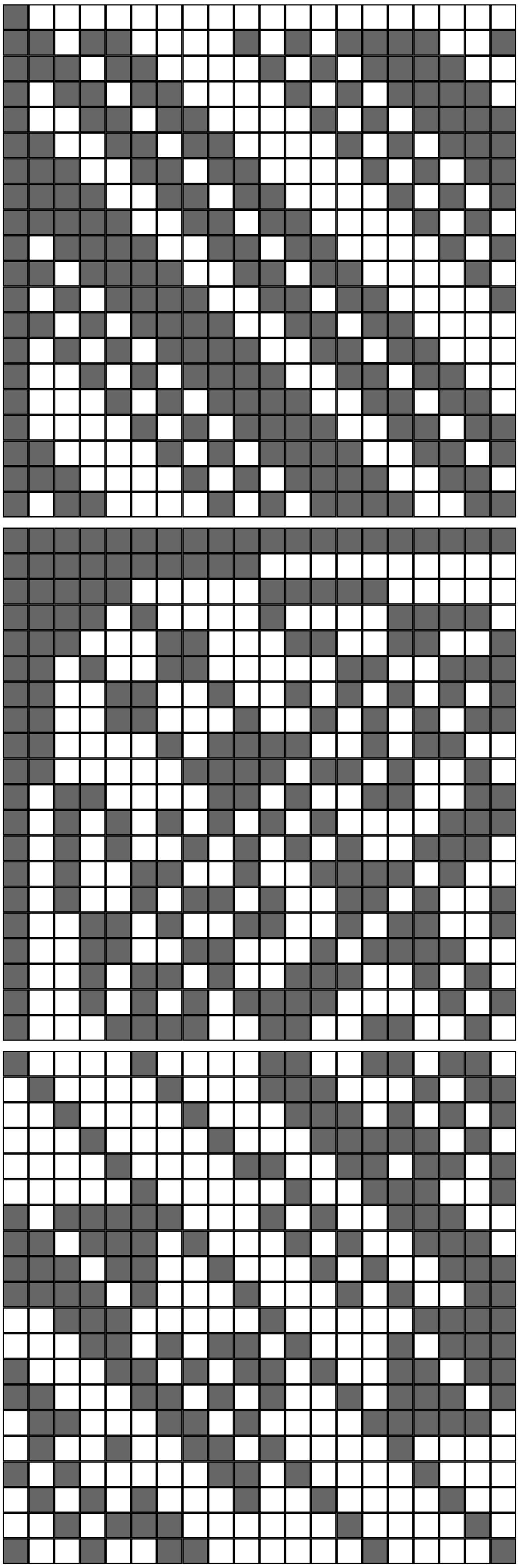
2. ***Paley inşası*** diye bilinen ve daha genel bir sonuç vardır. $p > 2$ bir asal, t ve k pozitif doğal sayı ve $n = 2^t(p^k + 1)$ olsun. O zaman n'lik bir Hadamard matrisi vardır. Bu da 2^t'lik bir Hadamard matrisine yukarıdaki sonuç uygulanarak elde edilir. ♣

Marrero adlı bir matematikçi bir iki yıl önce bir Hadamard matrisinden üç yeni Hadamard matrisi türetmeyi başardı. Marrero'nun yöntemi şöyle: Herhangi bir $2m$'lik H Hadamard matrisi ele alalım (m çift olmalı). Eğer $J = J_{m\times 1}$, her girdisi 1 olan $m \times 1$'lik sütun vektörse, H'yi aşağıdaki gibi bir Hadamard matrisine dönüştürebiliriz.

$$\begin{pmatrix} J & J & A \\ J & -J & B \end{pmatrix}$$

Şimdi A ve B yerine $-A$ ve/ya da $-B$ alarak, aşağıdaki gibi üç yeni Hadamard matrisi elde edebiliriz:

$$\begin{pmatrix} J & J & -A \\ J & -J & B \end{pmatrix}, \begin{pmatrix} J & J & A \\ J & -J & -B \end{pmatrix}, \begin{pmatrix} J & J & -A \\ J & -J & -B \end{pmatrix}.$$



20x20'lik üç Hadamard matrisi,
0 yerine boş kare, 1 yerine gri kare konuldu.